BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 05. 2023 - 23. 05. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Jenkins CAS plugin - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	HPE produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	IBM InfoSphere - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Snap One OvrC Cloud - viacero bezpečnostných zraniteľností	Vysoká	**8.6**
06.	VMware Tanzu Spring Boot - bezpečnostná zraniteľnosť	Vysoká	**7.5**
07.	Mitsubishi Electric MELSEC WS Series - bezpečnostná zraniteľnosť	Vysoká	**7.5**
08.	Aruba EdgeConnect Enterprise - bezpečnostná zraniteľnosť	Vysoká	**7.2**
09.	Craft CMS - bezpečnostná zraniteľnosť	Vysoká	**7.2**
10.	RA FactoryTalk Vantagepoint a ArmorStart - viacero bezpečnostných zraniteľností	Vysoká	**7.1**
11.	MicroSCADA Pro/X SYS600 - bezpečnostná zraniteľnosť	Stredná	**6.7**
12.	KeePass - bezpečnostná zraniteľnosť	Stredná	**6.2**
13.	Pimcore - bezpečnostná zraniteľnosť	Stredná	**6.2**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01794/2022/SK-CERT-1155

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Jenkins CAS plugin - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu CAS pre Jenkins vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.05.2023

CVE

CVE-2023-32997

Zasiahnuté systémy

Jenkins CAS Plugin vo verzii staršej ako 1.6.3

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/255479

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

HPE produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie pre produkty HP-UX OpenSSL Software, HPE Cray Accelerator Blade a HPE ProLiant Server Blade, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte HPE Cray EX235a Accelerator Blade, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.05.2023

CVE

CVE-2021-26354, CVE-2021-26356, CVE-2021-26371, CVE-2021-26379, CVE-2021-46756, CVE-2021-46762, CVE-2021-46763, CVE-2021-46764, CVE-2021-46769, CVE-2021-46775, CVE-2022-33894, CVE-2022-38087, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-20520

Zasiahnuté systémy

Cray EX235a Accelerator Blade vo verzii staršej ako 1.6.2
HPC Firmware Pack (HFP) vo verzii staršej ako 23.05
HP-UX OpenSSL Software vo verzii staršej A.01.01.01t.001

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2021-46769
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04455en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04464en_us
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04475en_us

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.05.2023

CVE

CVE-2023-2721, CVE-2023-2722, CVE-2023-2723, CVE-2023-2724, CVE-2023-2725, CVE-2023-2726

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 113.0.5672.126

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://chromereleases.googleblog.com/2023/05/stable-channel-update-for-desktop_16.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/255458

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM InfoSphere - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu IBM InfoSphere Information Server.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.05.2023

CVE

CVE-2023-32336

Zasiahnuté systémy

InfoSphere Information Server vo verzii staršej ako 11.7 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú k dispozícii bezpečnostné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.ibm.com/support/pages/node/6995879
https://exchange.xforce.ibmcloud.com/vulnerabilities/255285

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Snap One OvrC Cloud - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Snap One vydala bezpečnostnú aktualizáciu na svoj produkt OvrC Cloud, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.05.2023

CVE

CVE-2023-25183, CVE-2023-28386, CVE-2023-28412, CVE-2023-28649, CVE-2023-31193, CVE-2023-31240, CVE-2023-31241, CVE-2023-31245

Zasiahnuté systémy

OvrC Pro vo verzii staršej ako 7.3

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že aktualizácia systému nie je možná, výrobca odporúča znefunkčniť UPnP.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-136-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware Tanzu Spring Boot - bezpečnostná zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt Tanzu Spring Boot, ktorá opravuje bezpečnostnú zraniteľnosť.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.05.2023

CVE

CVE-2023-20883

Zasiahnuté systémy

VMware Tanzu Spring Boot vo verziách starších ako 3.0.7 a 2.7.12

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://spring.io/security/cve-2023-20883
https://exchange.xforce.ibmcloud.com/vulnerabilities/255809

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric MELSEC WS Series - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Mitsubishi Electric MELSEC WS Series.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi pripojiť sa ilegálne k modulu cez Telnet a vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

18.05.2023

CVE

CVE-2023-1618

Zasiahnuté systémy

WS0-GETH00200 vo všetkých verziách

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame postupovať podľa pokynov výrobcu uvedených na odkaze v časti ZDROJE.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-002_en.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-138-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Aruba EdgeConnect Enterprise - bezpečnostná zraniteľnosť

Popis

Spoločnosť Aruba vydala bezpečnostnú aktualizáciu na svoj produkt EdgeConnect Enterprise, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.05.2023

CVE

CVE-2023-30503

Zasiahnuté systémy

Aruba EdgeConnect Enterprise vo verzii staršej ako 9.3.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/255533

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Craft CMS - bezpečnostná zraniteľnosť

Popis

Vývojári redakčného systému Craft vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.05.2023

CVE

CVE-2023-32679

Zasiahnuté systémy

Craft CMS vo verzii staršej ako 4.4.6

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Craft v zraniteľnej verzii. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://github.com/craftcms/cms/security/advisories/GHSA-vqxf-r9ph-cc9c

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

RA FactoryTalk Vantagepoint a ArmorStart - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt Automation FactoryTalk Vantagepoint, ktorá opravuje bezpečnostnú zraniteľnosť a zverejnila informácie o zraniteľnostiach produktu ArmorStart.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

16.05.2023

CVE

CVE-2023-2444, CVE-2023-29022, CVE-2023-29023, CVE-2023-29024, CVE-2023-29025, CVE-2023-29026, CVE-2023-29027, CVE-2023-29028, CVE-2023-29029, CVE-2023-29030, CVE-2023-29031

Zasiahnuté systémy

FactoryTalk Vantagepoint: All versions prior to 8.40

ArmorStart ST281E, ST284E a ST280E vo všetkých verziách

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-136-03

https://www.cisa.gov/news-events/ics-advisories/icsa-23-136-02

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

MicroSCADA Pro/X SYS600 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Hitachi Energy vydala bezpečnostnú aktualizáciu na svoj produkt MicroSCADA Pro/X SYS600, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.05.2023

CVE

CVE-2011-1207

Zasiahnuté systémy

MicroSCADA Pro/X SYS600 vo verzii staršej ako 10.2

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=8DBD000142
https://www.cisa.gov/news-events/ics-advisories/icsa-23-138-03

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

KeePass - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti nástroja pre správu hesiel KeePass. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom. Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

15.05.2023

CVE

CVE-2023-32784

Zasiahnuté systémy

KeePass vo verzii staršej ako 2.54

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://github.com/vdohney/keepass-password-dumper
https://sourceforge.net/p/keepass/discussion/329220/thread/f3438e6283/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Pimcore - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Pimcore vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej GET požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

22.05.2023

CVE

CVE-2023-28438

Zasiahnuté systémy

Pimcore vo verzii staršej ako 10.5.19

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.sonarsource.com/blog/pimcore-one-click-two-security-vulnerabilities/
https://exchange.xforce.ibmcloud.com/vulnerabilities/250778
https://www.securityweek.com/pimcore-platform-flaws-exposed-users-to-code-execution/